IN THE CLAIMS

Please amend the claims to read as follows:

Listing of Claims

1. (Currently Amended) A system for transferring proprietary information through a communications pipe established between at least a first remote computer system and at least a personal security device using a local client as a communications host for said personal security device, said system comprising:

at least one network, wherein said network includes means for functionally connecting at least one local client with said at least one first remote computer system;

said local client further comprising means for functionally connecting to a personal security device Interface and said network, means for functionally communicating over said network with said remote computer system and means for establishing a communications pipe, said means for establishing a communications pipe comprising:

client communications means for transmitting and receiving message packets over said network using a packet based communications protocol, and for transmitting and receiving application protocol data units (APDUs) through said personal security device Interface;

first client data processing means for receiving incoming message packets from said remote computer system using said client communications means, separating encapsulated APDUs from said incoming message packets thus generating desencapsulated APDUs and routing said desencapsulated APDUs to said personal security device through said personal security device Interface independently of the origin and integrity of said incoming message packets; and

second client data processing means for receiving incoming APDUs from said personal security device interface, encapsulating said incoming APDUs into outgoing message packets and routing said outgoing message packets to said remote computer system through said client communications means;

said at least one personal security device further comprising at least one embedded personal security device application, a microprocessor, a runtime environment and at least one internal memory location, wherein said embedded application receives proprietary information through said established communications pipe and stores said information in said internal memory location and wherein said personal security device is functionally connected to said client and is functionally

communicating with said client and said first remote computer system through said established communications pipe; and

said at least one first remote computer system further comprising means for transferring said proprietary information from a storage location through said established communications pipe, wherein said first remote computer system is functionally connected to said network and is functionally communicating with said client and said personal security device through said established communications pipe.

2. (Previously Presented) The system according to claim 1, further comprising cryptography means for decrypting encrypted said incoming proprietary information and encrypting outgoing responses communicated through said established communications pipe.

3. (Original) The system according to claim 1, wherein said memory location is an open location.

4. (Original) The system according to claim 1, wherein said memory location is a secure location.

5. (Previously Presented) The system according to claim 1, further comprising receiving, processing and routing means for transferring said proprietary information received over said network from at least one subsequent remote computer system through said established communications pipe to said personal security device.

6. (Original) The system according to claim 1, wherein said storage location is local to said first remote computer system.

7. (Original) The system according to claim 1, wherein said storage location is local to at least one subsequent remote computer system.

8. (Original) The system according to claim 1, further comprising means for functionally connecting said first remote computer system with at least one subsequent remote computer system.

9. (Original) The system according to claim 8, wherein said subsequent remote computer system is functionally connected

to said network and is functionally communicating with said first remote computer system using said network.

10. (Previously Presented) The system according to claim 1, wherein said established communications pipe employs an open communications protocol.

11. (Previously Presented) The system according to claim 1, wherein said established communications pipe employs a secure communications protocol.

12. (Currently Amended) A method for transferring proprietary information through a communications pipe between at least a first remote computer system and at least a personal security device using a local client as a communications host for said personal security device, said method comprising:

establishing a communications pipe between said personal security device and said first remote computer system over at least one network and using said client as a communications host for said personal security device, wherein said client and said remote computer system are in functional communication using a packet based communications protocol over said network, and wherein transmitting a message from said remote computer system

to said personal security device through said communications pipe comprises:

generating a message on said remote computer system, wherein said message is in a non-native protocol for communicating with said personal security device and said message is generated by an API Level Program,

converting on said remote computer system said message from said non-native protocol into an application protocol data unit (APDU) format message using a first server data processing means,

encapsulating on said remote computer system said APDU format message into said packet based communications protocol producing an encapsulated message, using a second server data processing means,

transmitting said encapsulated message over said network using said packet based communications protocol,

receiving by said client said encapsulated message sent over said network, processing said encapsulated message using a first data processing means to separate said APDU format message from said encapsulated message, and

routing on said client said APDU format message through a hardware device port assigned to a personal security device Interface, independently of the origin and integrity

of said encapsulated message, wherein said personal security device Interface is in processing communication with said personal security device;

retrieving said proprietary information from a storage location by said first remote computer system,

processing said proprietary information by said first remote computer system,

transmitting as a message said proprietary information through said established communications pipe to said personal security device,

receiving said proprietary information through said established communications pipe from said first remote computer system by said personal security device, and

storing said proprietary information in a memory location inside said personal security device, using at least one embedded internal algorithm.

13. (Original) The method according to claim 12, further comprising retrieving said proprietary information from a local storage location.

14. (Original) The method according to claim 12, further comprising retrieving said proprietary information from a remote storage location.

15. (Original) The method according to claim 12, further comprising establishing said communications pipe using an open communications protocol.

16. (Original) The method according to claim 12, further comprising establishing said communications pipe using a secure communications protocol.

17. (Currently Amended) A method for transferring proprietary information through a communications pipe between at least a first remote computer system and at least a personal security device using a local client as a communications host for said personal security device, said method comprising:

establishing a communications pipe between said personal security device and said first remote computer system over at least one first network and using said client as a communications host for said personal security device, wherein said client and said remote computer system are in functional communication using a packet based communications protocol over said network, and

wherein transmitting a message from said remote computer system to said personal security device through said established communications pipe comprises:

generating a message on said remote computer system, wherein said message is in a non-native protocol for communicating with said personal security device and said message is generated by an API Level Program,

converting on said remote computer system said message from said non-native protocol into an application protocol data unit (APDU) format message using a first server data processing means,

encapsulating on said remote computer system said APDU format message into said packet based communications protocol producing an encapsulated message, using a second server data processing means,

transmitting said encapsulated message over said network using said packet based communications protocol,

receiving by said client said encapsulated message sent over said network, processing said encapsulated message using a first data processing means to separate said APDU format message from said encapsulated message, and

routing on said client said APDU format message through a hardware device port assigned to a personal security

device Interface independently of the origin and integrity of said encapsulated message, wherein said personal security device Interface is in processing communication with said personal security device;

establishing communications between said first remote computer system and a subsequent remote computer system over at least one second network,

transmitting said proprietary information over said at least one second network by said at least one subsequent remote computer system,

receiving said proprietary information sent over said at least one second network by said at least one subsequent remote computer system,

processing said proprietary information by said first remote computer system,

transmitting as a message said proprietary information through said established communications pipe to said personal security device,

receiving said proprietary information through said established communications pipe from said first remote computer system by said personal security device, and

storing said proprietary information in a memory location inside said personal security device, using at least one embedded internal algorithm.

18. (Original) The method according to claim 17, further comprising establishing said communications pipe using an open communications protocol.

19. (Original) The method according to claim 17, further comprising establishing said communications pipe using a secure communications protocol.

20. (Original) The method according to claim 17, further comprising establishing said communications using an open communications protocol.

21. (Original) The method according to claim 17, further comprising establishing said communications using a secure communications protocol.

22. (Previously Presented) The method according to claim 12 or claim 17, further comprising;

encrypting said proprietary information by said first remote computer system prior to transmitting said proprietary information through said established communications pipe, and

decrypting said encrypted proprietary information after receiving said proprietary information through said established communications pipe by said personal security device.

23. (Original) The method according to claim 22 further comprising;

encrypting said proprietary information by said subsequent remote computer system prior to transmitting said proprietary information over said communications network, and

decrypting said encrypted proprietary information after receiving said proprietary information over said network by said first remote computer system.